JOURNAL OF NUMBER THEORY **59**, 88–105 (1996)
ARTICLE NO. 0089

Dickson Polynomial Discriminators

PIETER MOREE*

Max-Planck Institut für Mathematik,
Gottfried-Claren Strasse 26, 53225 Bonn, Germany

AND

GARY L. MULLEN[†, ‡]

Mathematics Department, The Pennsylvania State University,
University Park, Pennsylvania 16802

For an integer a the integral Dickson polynomial of degree $j \geqslant 1$ is defined by

$$g_j(X, a) = \sum_{i=0}^{[j/2]} \frac{j}{j-i} \binom{j-i}{i} (-a)^i X^{j-2i}.$$

We consider the Dickson discriminator problem, that is we study the problem of finding for all integers a and all natural numbers j and n, the smallest positive integer k for which the integers $g_j(1, a), g_j(2, a), ..., g_j(n, a)$ are distinct modulo k.

1. INTRODUCTION

Given positive integers j and n, the discriminator $D(j, n)$ is defined to be the smallest positive integer k for which the first n, jth powers $1^j, 2^j, ..., n^j$ are distinct modulo k. This function was first introduced in the $j=2$ case by Arnold, Benkoski and McCabe [1] in developing an algorithm to quickly calculate square roots of a long sequence of integers. More recently Schumer [20] considered the cases where $j=3$ and 6, and in [21] Schumer and Steinig considered the case $j=2^h$ for $h \geqslant 2$. Barcau [2] resolved the case where j is an odd prime.

* Supported by the Netherlands Organization for Scientific Research (NWO). E-mail: moree@mpim-bonn.mpg.de.

† This author would like to thank the National Security Agency for partial support under Grant MDA904-92-H-3044.

‡ E-mail: mullen@math.psu.edu.

0022-314X/96 $18.00

Let φ denote Euler's totient function and let (a, b) denote the greatest common divisor of the integers a and b. For fixed j, in [4] Bremser, Schumer and Washington resolved the discriminator problem for all sufficiently large n by proving.

THEOREM 1. (i) *Let $j \geqslant 3$ be odd and let B_j be the smallest integer such that for all $n \geqslant B_j$, there exists a prime p with $(p-1, j) = 1$ and $n \leqslant p < 4n/3$. Then for $n \geqslant B_j$, $D(j, n) = \min\{k \mid k \geqslant n,\ k$ squarefree, $(\varphi(k), j) = 1\}$.*

(ii) *Let j be even and let C_j be the smallest integer $\geqslant 19$ such that for all $n \geqslant C_j$, there exists a prime p with $(p-1, j) = 2$ and $2n < p < 3n$. Then for $n \geqslant C_j$, $D(j, n) = \min\{k \mid k \geqslant 2n,\ k = q$ or $2q$, q prime, $(\varphi(k), j) = 2\}$.*

It appears from the papers referred to so far that the authors were either unaware of, or at least did not explicitly mention, the rather obvious connection between the discriminator problem and permutation polynomial results over the ring Z/kZ of integers modulo k. It has been known for many years (see W. Nöbauer [18]), that X^j $(j > 1)$ induces a permutation on Z/kZ if and only if k is squarefree and $(j, \varphi(k)) = 1$. Clearly if $k \geqslant n$ and X^j permutes Z/kZ, then $f(1), ..., f(n)$ are distinct modulo k. Thus as an immediate consequence we have that

$$\begin{aligned} D(j, n) &\leqslant \min\{k \mid k \geqslant n,\ X^j \text{ permutes } Z/kZ\} \\ &= \min\{k \mid k \geqslant n,\ k \text{ squarefree},\ (j, \varphi(k)) = 1\}. \end{aligned}$$

The difficult part of proving Theorem 1, (i) for example, is thus the reverse inequality. Similarly for j even, one would like to have an interpretation for the condition appearing in Theorem 1(ii). Since $x^j \equiv (-x)^j \pmod{k}$, x^j can not be a permutation polynomial over Z/kZ, however, it can be a *weak permutation polynomial* in the sense that it has the property that for arbitrary positive integers r and s, $r^j \equiv s^j \pmod{k}$, implies $r \equiv \pm s \pmod{k}$. Indeed, it turns out that for $k \geqslant 11$, X^j with j even is a weak permutation polynomial if and only if $k = q$ or $k = 2q$, with q prime and $(\varphi(k), j) = 2$. See Section 5 for more on weak permutation polynomials.

A generalization of the cyclic polynomials is given by Dickson (Chebyshev) polynomials. The integral Dickson polynomial $g_j(X, a)$ of degree $j \geqslant 1$ and parameter $a \in Z$ is defined by

$$g_j(X, a) = \sum_{i=0}^{[j/2]} \frac{j}{j-i} \binom{j-i}{i} (-a)^i X^{j-2i},$$

where [ ] denotes the greatest integer function. Note that $g_j(X, 0) = X^j$. It can be shown that $g_j(X, a) \in Z[X]$. While Dickson polynomials appear to

be much more complicated that the power or cyclic polynomials X^j, they are, via their functional equation P4 of Lemma 7 below, reasonably easy to work with.

For given positive integers j and n and an integer a, we define the Dickson discriminator $Dickson_a(j, n)$ to be the smallest positive integer k for which the integers $g_j(1, a), g_j(2, a), ..., g_j(n, a)$ are distinct modulo k. If $g_j(r, a) = g_j(s, a)$ for some $1 \leqslant r < s \leqslant n$, we put $Dickson_a(j, n) = \infty$. Notice that $Dickson_0(j, n) = D(j, n)$.

We obtain results (Theorems 9 and 16) for the Dickson polynomial $g_j(X, a)$ analogous to those of Theorem 1 for the power polynomial X^j. The difference is that in the case when j is odd the condition on k aside from the condition including both j and k, is much less restrictive than the corresponding condition for the power polynomial X^j. The reason for this is that Dickson polynomials can permute elements of rings Z/kZ with $k = p^e$ and $e \geqslant 2$. A polynomial of the form X^j with $j > 1$ never permutes the elements of rings of this form. We also note that if a polynomial permutes Z/p^2Z, it also permutes Z/p^eZ for every $e \geqslant 2$. The upshot is that unlike the power polynomial case, we now have to investigate the action of Dickson polynomials on rings of the form Z/p^eZ with $e \geqslant 2$. In order to apply the functional equation P4 below, we have to study rings that are quadratic extensions of the above rings. These are special cases of Galois rings, finite algebraic extensions of rings of the form Z/p^eZ with $e \geqslant 1$. The fact that, in contrast to the discriminator case, enough non squarefree numbers occur as images, makes it possible to give a characterization of $Dickson_a(j, n)$ with $(6, j) = 1$ and $6 \nmid a$, for all $n \geqslant 1$ (Theorem 9). For the remaining values of j, $g_j(X, a)$ is not a permutation polynomial on the field F_p for infinitely many primes p. From [12, Exer. 3.16] or from Dirichlet's theorem on primes in an arithmetic progression, it is known that X^j permutes F_p for infinitely many primes p if and only if $(j, 2) = 1$. Analogously ([12, Exer. 3.17] or Dirichlet's theorem), it is known for $a \neq 0$ that $g_j(X, a)$ induces a permutation on the field F_p for infinitely many primes p if and only if $(j, 6) = 1$. In particular in the cases $j \equiv 2, 10 \pmod{12}$, $g_j(X, a)$ does not permute F_p for infinitely many primes p; however, in these cases $g_j(X, a)$ is nearly a permutation polynomial in the sense that if $(a, p) = 1$ and $(j, p^{2m} - 1) = 2$, then $g_j(x, a) = g_j(y, a)$ implies $x = y$ or $x = -y$ over the field F_{p^m}. This turns out to suffice to derive a characterization of the Dickson discriminator in these cases too (Theorem 16). In Section 5 we return to polynomials with this type of property.

Based on the growth of the image of the Dickson discriminator $Dickson_a(j, n)$ for fixed j, we will introduce in Section 4 a measure of permutability. These growth considerations show that asymptotically Dickson polynomials are not better permuters than power polynomials of the same degree.

There are several reasons for studying the Dickson discriminator problem, including the fact that Dickson polynomials are known to play very important roles in the theory of permutation polynomials over finite fields. While it has been known for many years that Dickson polynomials have numerous applications in finite field theory, the fundamental role played by Dickson polynomials in the theory of permutations was first delineated by Fried in his proof [9] of the long standing Schur conjecture from 1923 concerning integral polynomials which induce permutations on the field F_p for infinitely many primes p, see Schur [22]. More recently their importance has again been realized through the proof [10] by Fried, Guralnick and Saxl of the Carlitz conjecture concerning permutations of even degree over sufficiently large fields of odd order. Via his proof of one of the Chowla–Zassenhaus conjectures from [6], it has also recently been shown by Cohen [7] that for p a sufficiently large prime, all permutations of small degree come from Dickson polynomials.

Given a polynomial f over the finite field F_q of order q, it is in general very difficult to determine the cardinality of the value set $V_f = \{f(\alpha) \mid \alpha \in F_q\}$ of f. This is easy for the power polynomial X^j, in fact $|V_{X^j}| = (q-1)/d+1$ where $d=(q-1, j)$. In [5] the cardinality of the value set of the Dickson polynomial $g_j(X, a)$ of degree j was determined and since this result will be used later, we state this as

LEMMA 2. *If q is odd with $2^r \| (q^2-1)$, then for each $j \geqslant 1$ and each $a \in F_q^*$, we have*

$$|V_{g_j(X,a)}| = \frac{q-1}{2(j, q-1)} + \frac{q+1}{2(j, q+1)} + \alpha,$$

where $\alpha = 1$; $1/2$; 0 respectively if $2^{r-1} \| j$ and a is a non-square; if $2^t \| j$ with $1 \leqslant t \leqslant r-2$; otherwise.

See also Bremser and Gomez-Calderon [3] for analogous Dickson polynomial results over more general Galois rings. It is because of the importance of Dickson polynomials in all of the above permutational type problems that we consider a Dickson discriminator function.

In [16] the discriminator for arbitrary $f \in Z[X]$ is considered. Criteria on f are given such that $D_f(n)$, defined to be the smallest positive integer k for which $f(1), ..., f(n)$ are distinct modulo k, satisfies

$$D_f(n) = \min\{k \mid k \geqslant n, f \text{ permutes } Z/kZ\},$$

for all n sufficiently large. In particular cyclic and Dickson polynomials with j odd, respectively $(6, j) = 1$ satisfy the criteria, however, except for the cyclic case, the resulting theorem is not as strong as the theorem given in

this paper (Theorem 9). A further refinement of the criteria for an arbitrary polynomial f is given in [24]. Specializing the method of proof of [16] to Dickson polynomials, yields a quite distinct proof of (a weaker version of) Theorem 9. A main ingredient is Wan's upper bound [23] for the value set of non-permutational polynomials.

2. Discriminators Revisited

Our main result (Theorem 9) depends on an improvement of the $4n/3$ in Theorem 1(i) which has some interesting consequences for the discriminator as well, that are pointed out in Theorem 3 and Example 4 (both were independently discovered by M. Zieve).

Theorem 3. *Let $j>1$ be odd. For $n\geqslant 1$ put*

$$C(j,n)=\min\{k\,|\,k\geqslant n,\ k \text{ squarefree}, (\varphi(k),j)=1\}.$$

If $C(j,n)\leqslant 2n-5/2+(-1)^n/2$, then

$$D(j,n)=C(j,n). \tag{1}$$

In particular (1) *holds if $n\leqslant 2^{33}-2$ $(=2\cdot 3\cdot 5\cdot 17\cdot 257\cdot 65537)$.*

Thus the $4n/3$ in Theorem 1(i) can be replaced by $2n-1$. The following example shows that the number $2^{33}-2$ in Theorem 3 is the largest number m such that (1) holds for all $1\leqslant n\leqslant m$ and all odd $j>1$.

Example 4. *Let j be the greatest odd squarefree divisor of $\varphi(2^{33}-1)\cdots\varphi(2^{34}-3)$, then $D(j,2^{33}-1)=2\cdot(2^{33}-2)\neq C(j,2^{33}-1)$.*

In case j is even many examples which show that the characterization given in Theorem 1(ii) is not best possible exist already for $n=4$ [17], the smallest one being $D(2,4)=9$. In order to prove Theorem 3 we will need two lemmas. They sharpen Lemmas 2 and 3 of [4].

Lemma 5. *Let $j>1$. Suppose that $2\leqslant m\leqslant 2n-3$ and that m is not squarefree. Then there exist integers r and s, with $1\leqslant r<s\leqslant n$ such that $r^j\equiv s^j \pmod m$. If in addition n is even, then $2n-3$ can be improved to $2n-2$.*

Proof. Write $m=q^2t$, where $q\geqslant 2$. Let $r=q$ and $s=q+qt$. Then $r^j\equiv s^j \pmod m$. We have to show that $s\leqslant n$. If not, then $s/m=q(1+t)/q^2t>n/m>1/2$, so $1+1/t>q/2$. Hence $q<4$, so $q=3$ and $t=1$ or $q=2$ and $t\geqslant 1$. In the first case $s=6$ and $m=9\leqslant 2n-3$, so $s\leqslant n$. In the second case

$s = 2 + 2t$. Since $m = 4t \leqslant 2n - 3$, implies $m \leqslant 2n - 4$, it follows that $s \leqslant n$. The proof of the last part of the assertion is left to the reader.

On noting that the upper bound $4n/3$ in Lemma 3 of [4] can by replaced by $2n + 3$, we obtain the following result:

LEMMA 6. *Let $j > 1$ be odd. Suppose $m \leqslant 2n + 2$, m is squarefree, and there is a prime q dividing m such that $(q - 1, j) \neq 1$. Then there exist integers r and s, with $1 \leqslant r < s \leqslant n$, such that $r^j \equiv s^j \pmod m$.*

Proof of Theorem 3. Put $D(j, n) = m$. By the Box Principle $m \geqslant n$ and furthermore (cf. Introduction) $m \leqslant C(j, n)$. Now suppose that $m < C(j, n) \leqslant 2n - 5/2 + (-1)^n/2$. The conditions on m of either Lemma 5 or Lemma 6 are satisfied and hence there are $1 \leqslant r < s \leqslant n$ such that $r^j \equiv s^j \pmod m$. This contradicts $m = D(j, n)$. Thus $D(j, n) = C(j, n)$. To prove the latter part of Theorem 3, put $w = 2 \cdot 3 \cdot 5 \cdot 17 \cdot 257 \cdot 65537$. Notice that $C(j, n) \leqslant d$ for any divisor d of w satisfying $d \geqslant n$. Calculation shows that for every $3 \leqslant n \leqslant w$, the interval $[n, 2n - 5/2 + (-1)^n/2]$ contains at least one divisor of m. Since clearly $D(j, 1) = 1 = C(j, 1)$ and $D(j, 2) = 2 = C(j, 2)$, Theorem 3 follows.

Proof of Example 4. Let w be as in the proof of Theorem 3. It is well known that an odd prime p such that $p - 1$ is a power of 2 must be a Fermat prime, i.e. is a prime of the form $2^{2^i} + 1$ for some $i \geqslant 0$. From this it is easily deduced that $\varphi(k)$ is a power of 2 for some squarefree integer $k > 1$ if and only if k is a squarefree product of Fermat primes or two times such a product. Using this and the fact that $2^{32} + 1$ is not a prime, it follows that there is no squarefree k in $(w, 2w)$ such that $\varphi(k)$ is a power of two. The choice of j now ensures there is no squarefree integer k in $(w, 2w)$ such that $(\varphi(k), j) \neq 1$. Using Lemmas 5 and 6 it follows that $D(j, w + 1) \geqslant 2w$. We finish the proof by showing that there are no $1 \leqslant r < s \leqslant w + 1$ such that $r^j \equiv s^j \pmod{2w}$ (this together with $D(j, w + 1) \geqslant 2w$ implies $D(j, w + 1) = 2w$.) To this end assume that such r and s do exist. Since X^j permutes Z/wZ it follows that $r \equiv s \pmod w$. So $r = 1$ and $s = w + 1$. However, $1^j \not\equiv (1 + w)^j \equiv 1 + w \pmod{2w}$.

3. DICKSON DISCRIMINATORS

We now state several elementary but useful properties of Dickson polynomials, proofs of which can be found in [12, Chp. 2]. Property P4 is known as the functional equation and is one of the most important properties of Dickson polynomials.

LEMMA 7. *For each* $j \geqslant 1$

(P1) $g_{j+1}(X, a) = Xg_j(X, a) - ag_{j-1}(X, a)$, *with* $g_0(X, a) = 2$, $g_1(X, a) = X$.

(P2) $g_{2j}(X, a) = g_j(X, a)^2 - 2a^j$.

(P3) $g_j(-X, a) = (-1)^j g_j(X, a)$.

(P4) *If* $x = y + a/y$, *then* $g_j(x, a) = g_j(y + a/y, a) = y^j + (a/y)^j$.

(P5) $g_{jk}(X, a) = g_j(g_k(X, a), a^k)$ *for all positive integers* j *and* k.

(P6)

$$g_j(X, a) = \left(\frac{X + \sqrt{X^2 - 4a}}{2}\right)^j + \left(\frac{X - \sqrt{X^2 - 4a}}{2}\right)^j.$$

The next proposition shows that $Dickson_a(j, n)$ respects the multiplicative ordering of the integers in the first variable and the standard ordering in the second.

PROPOSITION 8. *For each integer* a

(i) $Dickson_a(j, n) \leqslant Dickson_a(j, m)$ *for all positive integers* n, m *with* $n \leqslant m$.

(ii) $Dickson_a(jk, n) \geqslant Dickson_a(j, n)$ *for all positive integers* j, k *and* n.

Proof. Clearly (i) holds. For (ii), if $n = 1$, the inequality clearly holds, so we assume $n \geqslant 2$. If $Dickson_a(j, n) = \infty$, then $g_j(r, a) = g_j(s, a)$ for some $1 \leqslant r < s \leqslant n$. Using property P5 of Lemma 7, it follows that $Dickson_a(jk, n) = \infty$. We may thus assume that $Dickson_a(jk, n) = m < Dickson_a(j, n) < \infty$. By definition of $Dickson_a(j, n)$, it follows that there are $1 \leqslant r < s \leqslant n$, such that $g_j(r, a) \equiv g_j(s, a) \pmod m$. Using P5 again it follows that $g_{jk}(r, a) \equiv g_{jk}(s, a) \pmod m$, contradicting the definition of m.

Not surprisingly the behaviour of $Dickson_a(j, n)$ for fixed j is quite different from that for fixed n. On the latter further details can be found in [17] in case $a = 0$

We define $\psi_a(k)$ to be $\varphi(k) \prod_{p|k,\, p \nmid a} (p + 1)$ ($\psi_0(k) := \varphi(k)$). The arithmetic function $\psi_1(k)$ was introduced by Nöbauer [18]. Of course $\psi_{-1}(k) = \psi_1(k) = \varphi(k) \prod_{p|k} (p + 1)$ and $\psi_a(k) \mid \psi_1(k)$ for each a. If $k = \prod_{p_i|k} p_i^{e_i}$, the a-part of k is defined as $\prod_{p_i|a,\, p_i|k} p_i^{e_i}$. (The 0-part of k we define to be k.)

3.1. *The Case Where j is Odd*

We now state the Dickson analogue of Theorem 3.

THEOREM 9. *Let $j>1$ be odd with $3 \nmid j$. For $n \geqslant 1$ and a an integer, put*

$$G_a(j, n) = \min\{k \geqslant n \mid (j, \psi_a(k)) = 1 \text{ and the } a\text{-part of } k \text{ is squarefree}\}.$$

If $G_a(j, n) \leqslant 2n - 5/2 + (-1)^n/2$, then

$$Dickson_a(j, n) = G_a(j, n). \tag{2}$$

In particular (2) holds if

(i) $n \leqslant 3570$,

(ii) *n is sufficiently large*,

(iii) $6 \nmid a$ *and* $n \geqslant 1$.

The following example shows that the number 3570 in (i) (take $\alpha = 1$) and the number 6 in (iii) are best possible for (2) to hold.

EXAMPLE 10. *Let Q denote the set of primes q not in $\{2, 3, 5, 7, 17\}$ such that $q-1$ has no prime factors outside the set $\{2, 3\}$. Let $\alpha \geqslant 1$ be arbitrary. Put $v = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 17 \cdot \prod_{p \mid \alpha,\, p \in Q} p$. Let j be the greatest squarefree divisor of $\psi_{6\alpha}(v+1) \cdots \psi_{6\alpha}(2v-1)$ coprime with 6. Then $Dickson_{6\alpha}(j, v+1) = 2v \neq G_{6\alpha}(j, v+1)$.*

We will prove the equality of Theorem 9 by showing that each side of (2) is at most equal to the other. As with the original discriminator problem, one direction (see Lemma 12) is rather trivial and follows easily from well known results concerning permutation polynomials. Part (i) of Lemma 13 and in particular part (ii) of Lemma 13 are the most difficult steps in the proof of the reverse inequality. Before giving the proof of Theorem 9, we establish some required lemmas.

LEMMA 11. *Let $k = \prod_{p_i \mid k} p_i^{e_i}$ be a natural number.*

(i) *If k is not squarefree, then the only permutation polynomial mod k of the form X^j is X, otherwise X^j is a permutation polynomial if and only if $(j, \varphi(k)) = 1$.*

(ii) *The polynomial $g_j(X, a)$ with $a \neq 0$ an integer and $gcd(a, k) = 1$, is a permutation polynomial mod k if and only if $(j, \psi_1(k)) = 1$.*

(iii) *For $j > 1$, $g_j(X, a)$ is a permutation polynomial mod k if and only if $(j, \psi_a(k)) = 1$ and the a-part of k is squarefree.*

Proof. Proofs of (i) and (ii) can be found in [12, Thms. 4.4, 4.5]. For (iii) it suffices to prove the assertion only in the case where k is a prime power, $k = p^e$, p prime. First we prove the necessity. If $p \nmid a$, it follows by part (ii) that $(j, p^{e-1}(p^2-1)) = 1$. If $p \mid a$ we must have $e = 1$, for in case

$e \geqslant 2$, $g_j(p^{e-1}, a) = g_j(0, a)$ over Z/p^eZ. By part (i) it follows that $(j, p-1) = 1$ on noting that $g_j(X, a) \equiv X^j \pmod a$. Conversely if $p \nmid a$, $(j, p^{e-1}(p^2-1)) = 1$ and so by part (ii), $g_j(X, a)$ permutes Z/p^eZ. If $p \mid a$, and $p^2 \nmid k$ then $e = 1$. Since $(j, p-1) = 1$ by assumption, it follows by (i) that $g_j(X, a)$ permutes Z/pZ, since over Z/pZ, $g_j(X, a) = X^j$.

Lemma 11 shows that if a contains many different prime factors, the behaviour of $g_j(X, a)$ becomes close to that of a power polynomial. So in some sense $g_j(X, -1)$ and $g_j(X, 1)$ are the most interesting Dickson polynomials. Note that parts (i) and (ii) of Lemma 11 are subcases of part (iii) in case $j > 1$.

LEMMA 12. *Let j be odd with $3 \nmid j$. Then $Dickson_a(j, n) \leqslant G_a(j, n) < \infty$. Furthermore $G_a(j, n) = n + o(n)$.*

Proof. By Dirichlet's Theorem, see Davenport [8, Chps. 20, 22], there exists a prime p exceeding n such that $p \equiv 2 \pmod j$. Using that $(j, p^2-1) = (j, 3) = 1$, we see that $G_a(j, n) \leqslant p < \infty$. Put $k = G_a(j, n)$. By Lemma 11 part (iii), $g_j(X, a)$ is a permutation polynomial over Z/kZ and so in particular $g_j(1, a), ..., g_j(n, a)$ are pairwise incongruent modulo k. It follows that $Dickson_a(j, n) \leqslant G_a(j, n)$. The latter part of the assertion follows on applying the prime number theorem for the arithmetic progression $2, 2+j, 2+2j, \ldots$ (see Davenport [8]).

LEMMA 13. *Let $j > 1$ be odd with $3 \nmid j$. Suppose that $m \leqslant 2n$ and that one of*

(i) *q divides m and $(q-1, j) \neq 1$*

(ii) *q divides m, q does not divide a and $(q+1, j) \neq 1$*

is satisfied for some prime q. Then $Dickson_a(j, n) \neq m$.

Proof. For $(y, m) = 1$, let $R(y)$ be the unique integer with $0 \leqslant R(y) < m$ such that $R(y) \equiv y + a/y \pmod m$. Let e be the exponent of q in m. Thus $m = q^e t$ with $(q, t) = 1$. Note that $q \geqslant 5$.

(i) Since by assumption j is odd, $3 \nmid j$ and $(q-1, j) \neq 1$, there is a prime $p \geqslant 5$ dividing $(q-1, j)$. The equation $x^p \equiv 1 \pmod q$ has distinct solutions $x'_1, ..., x'_p$. In the case $a^p \equiv 1 \pmod q$, the system of equations $x^2 = a$, $x^p = 1$, has one and only one solution $x = a^{(p+1)/2}$ over F_q, the finite field of order q. Denote it by x'_1. The other solutions of $x^p = 1$ can be arranged in such a way that $x'_{2i+1} \equiv a/x'_{2i} \pmod q$ for $i = 1, ..., (p-1)/2$. The solutions $x'_1, ..., x'_p$ can each be lifted to at least one solution modulo m, see for example [3, Lemma 1]. For $i = 1, ..., p$ choose a lifted value x_i of x'_i such that $x_i^p \equiv 1 \pmod m$. Notice that if $a^p = 1$ over F_q, none of the

x_i satisfies $x_i^2 = -a$. Otherwise there is at most one x_i, say x_p, satisfying $x_p^2 = -a$. In case $a^p = 1$, put $y = x_1$, $y_i = x_{2i-2}$ $(i = 2, ..., z)$, with $z = (p+1)/2$. Otherwise we put $y_i = x_i$ $(i = 1, ..., z)$ with $z = p-1$. Since $z \geqslant 3$, at least one of the following conditions is satisfied:

(1) there exist i, k $(i \neq k)$ with $R(y_i), R(y_k) < m/2$

(2) there exist i, k $(i \neq k)$ with $R(y_i), R(y_k) \geqslant m/2$.

In case (1) put $r = R(y_i)$ and $s = R(y_k)$. In case (2) put $r = m - R(y_i)$ and $s = m - R(y_k)$. Notice that both $r, s \leqslant m/2 \leqslant n$ and $r, s \geqslant 1$ (since $y_l^2 \not\equiv -a \pmod q$ for $l = 1, ..., z$). We have $y_i^j \equiv y_k^j \pmod m$ and on using properties P3 and P4 of Lemma 7 it follows that $g_j(r, a) \equiv g_j(s, a) \pmod m$, and thus $Dickson_a(j, n) \neq m$, provided we can show that $R(y_i) \neq R(y_k)$. It suffices to show that $R(y_i) \not\equiv R(y_k) \pmod q$ $(i < k)$, so assume that we have $R(y_i) = R(y_k)$ over F_q. If $i = 1$ and $a^p = 1$, $R(y_1) = 2a^{(p+1)/2} = R(y_k)$. But the equation $R(x)\, x = 2a^{(p+1)/2}x$ has $a^{(p+1)/2}$ as a root of multiplicity two. So $y_1 = y_k$ over F_q. This impossibility shows that $i \neq 1$ in case $a^p = 1$. If $i \neq 1$ and $a^p = 1$, $R(y_i) = R(y_k)$ would imply that the quadratic equation $xR(x) = xR(y_i)$ has four distinct solutions $(y_i, x_{2i-1}, y_k, x_{2k-1})$. This contradicts Lagrange's Theorem. In the remaining case $a^p \neq 1$, $R(y_i) = R(y_k)$ would imply $y_i y_k = a$ and thus $a^p = 1$.

(ii) Since $(q+1, j) \neq 1$, there is a prime $p \geqslant 5$ dividing both $q+1$ and j. We first consider the case where $e = 1$ and $t = 1$. We then work over the Galois ring $GR(q, 2) \cong F_{q^2}$. As is well-known $x^p = 1$ has p distinct solutions $x_1, ..., x_p$ ($x^p - 1$ divides $x^{q^2-1} - 1$). The equation $\gamma^{q+1} = a$ has $q+1$ distinct solutions $\gamma_1, ..., \gamma_{q+1}$ in F_{q^2}, and so a/γ^2 assumes $(q+1)/2$ different values. We distinguish two cases:

(A) $q + 1 > 2p$.

Choose a γ_i such that $(a/\gamma_i^2)^p \neq 1$, and put $\sigma = \gamma_i$. Notice that there is at most one k such that $(\sigma x_k)^2 = -a$. We can assume, without loss of generality, that $k = p$ (if such a k exists). Put $z = p - 1$. For $i = 1, ..., z$ we put $y_i = x_i$.

(B) $q + 1 = 2p$.

If there exists a γ_i such that $(a/\gamma_i^2)^p \neq 1$, we follow the procedure of case (A), otherwise there must exist a γ_j such that $a/\gamma_j^2 = 1$. Put $\sigma = \gamma_j$. Notice that in this case the system of equations

$$(\gamma x_i)^2 = -a, \qquad x_i^p = 1 \qquad \text{and} \qquad \gamma^{q+1} = a,$$

with a an integer not divisible by q, does not have solutions over F_{q^2}. We can reorder the roots of $x^p - 1$ so that $1, x_2, 1/x_2, ..., x_z, 1/x_z$ $(z = (p+1)/2)$ are all the p roots. Now put $y_1 = 1$, $y_i = x_i$ $(i = 2, ..., z)$.

For $i=1, ..., z$ we have, using the functional equation P4,

$$g_j(\sigma y_i + a/(\sigma y_i)) = g_j(\sigma + a/\sigma) = \sigma^j + (a/\sigma)^j.$$

Moreover $\sigma y_i + a/(\sigma y_i) = \sigma y_i + (\sigma y_i)^q \in Z/mZ$. The same conclusion holds of course for $\sigma + a/\sigma$ and for $\sigma^j + (a/\sigma)^j$. Since $z \geqslant 3$, at least one of the following conditions is satisfied:

(1) there exist i, k $(i \neq k)$ with $R(\sigma y_i), R(\sigma y_k) < m/2$.

(2) there exist i, k $(i \neq k)$ with $R(\sigma y_i), R(\sigma y_k) \geqslant m/2$.

In the first case put $r = R(\sigma y_i)$ and $s = R(\sigma y_k)$. In the second case put $r = m - R(\sigma y_i)$ and $s = m - R(\sigma y_k)$. Clearly $r, s \leqslant m/2 \leqslant n$. We have chosen the y_l so that $(\sigma y_l)^2 \neq -a$. Therefore r and s are $\geqslant 1$. We have to prove that $r \neq s$ in order to show that $Dickson_a(j, n) \neq m$. It suffices to show that $R(\sigma y_i) \neq R(\sigma y_k)$ over the ring $GR(q, 2)$. Now $R(\sigma y_i) = R(\sigma y_k)$ implies $y_i = y_k$ or $y_i = a/(\sigma^2 y_k)$. In the case $(a/\sigma^2)^p \neq 1$, it would follow that $y_i = y_k$, which is impossible. In the case $a/\sigma^2 = 1$, we also have a contradiction (since we have chosen the y_l so that $y_i \neq y_k$ and $y_i \neq 1/y_k$). This finishes the proof if $e = 1$ and $t = 1$.

In the general case first determine the y_i and σ in the subring $GR(q, 2)$. By the lifting lemma [3, Lemma 1], we can lift them to $y_1, ..., y_z, \sigma$ in $GR(q^e, 2)$. Recall that $GR(q^e, 2) \cong Z[X]/(q^e, f)$, for some monic basic irreducible polynomial $f(X)$ of degree 2. Let $\beta_1(X), ..., \beta_{z+1}(X)$ denote preimages of $y_1, ..., y_z, \sigma$ in $Z[X]$. Then $\beta_1(X)^q, ..., \beta_z(X)^q$ are preimages of $1/y_1, ..., 1/y_z$ in $Z[X]$. Now consider the ring $R = Z[X]/(m, f)$. Using the Chinese remainder theorem, we can find for $i = 1, ..., z+1$ a polynomial $\delta_i(X)$ such that $\delta_i(X) \equiv \beta_i(X) \pmod{q^e}$, and $\delta_i(X) \equiv 1 \pmod{t}$. The polynomials $\delta_i(X)$ are preimages of the lifted values of $y_1, ..., y_z, \sigma$ to R. Denote these lifted values by $y_1', ..., y_z', \sigma'$. Note that $y_1', ..., y_z'$ are solutions of $x^p = 1$ in R, but that σ' does not necessarily satisfy $(\sigma')^{q+1} = a$ in R. Let $\tau(X)$ be the preimage of a unit in R. Put $\delta(X) = \tau(X) + \tau(X)^q$ and notice that $\delta(X) = \delta(X)^q + q\sigma(X)$ for some $\sigma(X) \in Z[X]$. From this it follows that either $\delta(X)$ is a constant, or that $\delta(X) = qh(X)$ for some $h(X) \in Z[X]$, which is impossible since $\tau(X)$ is the preimage of a unit. It follows that $\delta(X) \in Z$ and therefore its image in R is in Z/mZ. Now consider the polynomial $\beta_{z+1}(X)\,\beta_i(X) + (\beta_{z+1}(X)\,\beta_i(X))^q$. Its image in R is $R(\sigma' y_i')$. Then by the above $R(\sigma' y_i') \in Z/mZ$. To show that $R(\sigma' y_i') \neq R(\sigma' y_k')$, it suffices to do so over the subring $GR(q, 2)$ of R. By restriction it is enough to show that $R(\sigma y_i) \neq R(\sigma y_k)$. Now proceed as in the case $e = 1$ and $t = 1$.

The following lemma is a Dickson analogue of Lemma 5.

LEMMA 14. *Let $j > 1$ be odd. Suppose $2 \leqslant m \leqslant 2n-3$, and that for some prime q, $q^2 | m$ and $q | ja$. Then there exist integers r and s, with $1 \leqslant r < s \leqslant n$*

such that $g_j(r, a) \equiv g_j(s, a) \pmod m$. *If in addition* n *is even, then* $2n-3$ *can be improved to* $2n-2$.

Proof. By the proof of Lemma 5, it suffices to check that $g_j(q, a) \equiv g_j(q+qt, a) \pmod m$ where $m = q^2 t$. Since $q^\alpha \equiv (q+qt)^\alpha \pmod m$ for $\alpha > 1$, we only have to show that $j(-a)^{(j-1)/2} q \equiv j(-a)^{(j-1)/2}(q+qt) \pmod m$. Since $q \mid ja$ by assumption, this is obvious.

Let $P(r)$ denote the greatest prime factor of r.

PROPOSITION 15. *The primes* 2, 3, 5, 7 *and* 17 *are the only primes such that* $P(p^2-1) \leqslant 3$.

Proof. This easily follows from the result of Levi ben Gerson (before 1350!), that if $3^m \pm 1 = 2^n$, then $m \leqslant 2$ (see Ribenboim [19, p. 5]).

Proof of Theorem 9. Put $Dickson_a(j, n) = m$. By the Box Principle $m \geqslant n$ and, by Lemma 12, $m \leqslant G_a(j, n)$. Now suppose that $m < G_a(j, n) \leqslant 2n - 2\frac{1}{2} + (-1)^n/2$. By the definitions of $G_a(j, n)$ and the function ψ_a, it follows that one of the conditions (i) or (ii) of Lemma 13 is satisfied, or that $q^2 \mid m$ and $q \mid ja$. By applying Lemmas 13 and 14 (respectively), we arrive at a contradiction. It follows that $Dickson_a(j, n) = G_a(j, n)$. For $n = 1$, 2 and 3, $G_a(j, n) = n$. By Lemma 12 and the Box Principle it follows that $Dickson_a(j, n) = G_a(j, n)$. So we may suppose that $n \geqslant 4$. On using that in the interval $[n, 2n - 5/2 + (-1)^n/2]$ there is a divisor m of 3570 and that $g_j(X, a)$ permutes $Z/3570Z$ (by Lemma 11(iii)), (i) is deduced (as $G_a(j, n) \leqslant m \leqslant 2n - 5/2 + (-1)^n/2$. Part (ii) follows by Lemma 12. By part (i) we may assume that $n \geqslant 3571$. In case $2 \nmid a$ we use that there is a number of the form $d \cdot 2^\alpha$ with $d = 1$, 3 or 5 in the interval $[n, 2n-3]$. In case $3 \nmid a$ we use that in the interval $[n, 2n-3]$ there is a number of the form $d \cdot 3^\alpha$ with $d = 1$, 5 or 7.

Remark 1. Note that the value of $G_a(j, n)$ depends only upon the squarefree part of both a and j.

Proof of Example 10. Using Proposition 15 it follows that the only solutions q, q prime $\geqslant 5$, and $e \geqslant 1$ of $P(\psi_{6\alpha}(q^e)) \leqslant 3$, are given by $e = 1$, $q = 5$, 7, 17 and the q dividing α that are in Q. Furthermore $P(\psi_{6\alpha}(2^e)) \leqslant 3$ and $P(\psi_{6\alpha}(3^e)) \leqslant 3$. Let k be a 6α-free integer in the interval $(v, 2v)$. Then, by the above and the multiplicativity of $\psi_{6\alpha}$, it follows that $P(\psi_{6\alpha}(k)) > 3$. The choice of j ensures that $(j, \psi_{6\alpha}(k)) > 1$. Using Lemma 11(iii) it follows that $g_j(X, 6\alpha)$ does not permute Z/kZ. Since this holds for any 6α-free integer k in $(v, 2v)$, it follows from the proof of Theorem 9 that $Dickson_{6\alpha}(j, v+1) \geqslant 2v$. We complete the proof by showing that $g_j(x, 6\alpha) \equiv g_j(y, 6\alpha) \pmod{2v}$, $1 \leqslant x \leqslant y \leqslant 1+v$ implies $x = y$. So assume that $x < y$. By Lemma 11(iii), $g_j(X, 6\alpha)$ permutes Z/vZ, so $x \equiv y \pmod v$.

Thus $x=1$, $y=1+v$. Using that $g_j(X, 6\alpha) \equiv X^j - 6j\alpha X^{j-2} \pmod 4$ we find that $g_j(1, 6\alpha) \not\equiv g_j(1+v, 6\alpha) \pmod 4$. To conclude the proof notice that $4 \nmid G_{6\alpha}(j, 1+v)$.

3.2. *The Case Where j is Even*

In this section we establish the Dickson analogue of Theorem 1(ii) in case $j \equiv 2 \pmod{12}$ or $j \equiv 10 \pmod{12}$. Using Lemma 18 and Dirichlet's Theorem the existence of $Dickson_a(j, n)$ is readily established. In the remaining case with j even, the existence of $Dickson_a(j, n)$ is not ensured (cf. Table 1).

THEOREM 16. *Suppose that* $j \equiv 2 \pmod{12}$ *or* $j \equiv 10 \pmod{12}$. *Let* L_j *be the smallest integer* $\geqslant \max\{19, P(a)+1\}$ *such that there is a prime* p *with* $2n < p \leqslant 10(n-3)/3$ *and* $(p^2-1, j) = 2$. *Then for* $n \geqslant L_j$,

$$Dickson_a(j, n) = \min\{k \geqslant 2n \mid (j, \psi_1(k)) = 2, k = p \text{ or } k = 2p, p \text{ prime}\}. \quad (3)$$

TABLE I

Dickson Discriminators

	n																			
j	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
2	1	2	6	9	10	13	14	17	19	22	22	26	26	29	31	34	34	37	38	41
3	1	3	3	7	11	13	13	13	33	33	39	39	59	59	71	71	71	71	71	103
4	1	2	7	10	14	14	17	26	29	53	53	53	62	62	62	62	89	94	94	94
5	1	2	3	4	5	6	7	8	9	10	12	12	13	14	15	16	17	18	20	20
6	1	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
7	1	2	3	4	5	6	7	8	9	10	11	12	14	14	15	16	17	18	19	20
8	1	2	10	10	17	26	26	26	29	53	53	53	74	74	89	89	101	101	101	101
9	1	3	3	7	11	13	13	13	33	33	39	39	59	59	79	79	79	79	79	103
10	1	2	6	9	10	13	14	17	23	23	23	26	26	34	34	34	34	37	43	43
11	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
12	1	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
13	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
14	1	2	6	9	10	14	14	17	19	22	22	31	31	31	31	34	34	37	38	46
15	1	3	3	7	13	13	13	13	39	39	39	39	69	69	97	97	97	97	103	103
16	1	2	10	10	18	26	26	26	29	53	53	53	74	74	89	89	101	101	101	101
17	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
18	1	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
19	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
20	1	2	7	10	14	14	17	26	53	53	53	53	73	74	94	94	94	94	94	94
21	1	3	3	7	11	19	21	24	33	33	59	59	59	59	79	79	79	79	79	103
22	1	2	6	9	10	13	14	17	19	22	22	26	26	29	31	34	34	37	38	41
23	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
24	1	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
25	1	2	3	4	5	6	7	8	9	10	12	12	13	14	15	16	17	18	20	20

Remark 2. On using the prime number theorem for the arithmetic progression $3, 3+j, 3+2j, \ldots$, it easily follows that L_j exists.

As with the proof of Theorem 9, the proof of Theorem 16 proceeds by establishing that each side of (3) is at most equal to the other. We commence by making a trivial observation.

PROPOSITION 17. *If j is even and $n \geqslant 3$, then $Dickson_a(j, n) \geqslant 2n$.*

Proof. Suppose $Dickson_a(j, n) = m < 2n$. Then, since $m \geqslant n$ and by assumption $n \geqslant 3$, there exist $1 \leqslant r < s \leqslant n$ such that $r + s = m$. Since $g_j(X, a)$ is in $Z[X^2]$, it follows that $g_j(r, a) \equiv g_j(s, a) \pmod{m}$.

Part of the proof of Theorem 16 follows from:

LEMMA 18. *Suppose $j \equiv 2 \pmod{12}$ or $j \equiv 10 \pmod{12}$ and $n \geqslant 3$. If $k \geqslant 2n$, $(j, \psi_1(k)) = 2$, and $k = p$ or $k = 2p$, p prime, then $Dickson_a(j, n) \leqslant k$.*

Proof. We only consider the case $k = 2p$, the case $k = p$ can be dealt with similarly (and is in fact easier). Suppose that $Dickson_a(j, n) > k$. Then there are $1 \leqslant r < s \leqslant n$ such that

(i) $g_j(r, a) \equiv g_j(s, a) \pmod{2}$

(ii) $g_j(r, a) \equiv g_j(s, a) \pmod{p}$.

By Lemma 11(iii) $g_j(X, a)$ permutes $Z/2Z$, so we deduce from (i) that $r \equiv s \pmod{2}$. Using properties P2 and P3 of Lemma 7, we deduce from (ii) that $g_{j/2}(r, a) \equiv g_{j/2}(s, a) \pmod{p}$ or $g_{j/2}(-r, a) \equiv g_{j/2}(s, a) \pmod{p}$. Since $(j/2, \psi_1(k)) = 1$ and so $(j/2, \psi_a(k)) = 1$ ($\psi_a(k)$ divides $\psi_1(k)$), it follows by Lemma 11(iii) that $r \equiv s \pmod{p}$ or $-r \equiv s \pmod{p}$ and so $r \equiv s \pmod{k}$ or $-r \equiv s \pmod{k}$ when $j > 2$ is even. In case $j = 2$ the same conclusion holds. Using that $1 \leqslant r < s \leqslant n$ and that $k \geqslant 2n$, it follows that $r = s$. This contradiction yields the truth of the lemma.

Proof of Theorem 16. Assume that $n \geqslant L_j \geqslant 10$. By Proposition 17, $Dickson_a(j, n) \geqslant 2n$. By the definition of L_j, there is a prime q between $2n$ and $10(n-3)/3$ with $(j, q^2 - 1) = 2$, so by Lemma 18, $Dickson_a(j, n) < 10(n-3)/3$. Put $Dickson_a(j, n) = k$ and suppose that k is neither a prime nor twice a prime. Then there exist r and s with $1 \leqslant r < s \leqslant n$ such that $r^2 \equiv s^2 \pmod{k}$; see the proof of Lemma 4 of Arnold, Benkoski and McCabe [1]. Since $g_j(X, a)$ is in $Z[X^2]$ it follows that $g_j(r, a) \equiv g_j(s, a) \pmod{k}$.

Now suppose $k = p$ or $2p$, p prime, $(j, \psi_1(k)) \neq 2$ and $2L_j \leqslant 2n \leqslant k < 10(n-3)/3$. Then $\max\{(p-1, j), (p+1, j)\} \geqslant 10$ and $\min\{(p-1, j), (p+1, j)\} = 2$. Notice that $p \nmid a$. In case $k = p$ we have using Lemma 2, $|V_{g_j(X, a)}|$ on $Z/kZ \leqslant (p-1)/20 + (p+1)/4 + 1 < n$. This shows that

$g_j(r, a) \equiv g_j(s, a) \pmod{k}$ for some $1 \leqslant r < s \leqslant n$. By using the Chinese remainder theorem and the observations made in the analysis of (i) of Lemma 18, in case $k = 2p$ we have $|V_{g_j(X,a)}|$ on $Z/kZ \leqslant 2\,|V_{g_j(X,a)}|$ on $Z/pZ \leqslant (p-1)/10 + (p+1)/2 + 2 < n$. Again it follows that $g_j(r, a) \equiv g_j(s, a) \pmod{k}$ for some $1 \leqslant r < s \leqslant n$. On using Lemma 18 it follows that k must satisfy the conditions of Theorem 16.

Remark 3. We note that if $j \equiv 2 \pmod{12}$ or $j \equiv 10 \pmod{12}$ and $n \geqslant \max\{C_j, L_j\}$, then $D(j, n) \leqslant Dickson_a(j, n)$. Furthermore there exists $n(a)$ such that $Dickson_a(j, n) = Dickson_1(j, n)$ for $n \geqslant n(a)$.

4. Growth of the Discriminator

We propose measures of permutability $\mu_D(j)$ and $\mu_P(j)$ based on the growth of the Dickson discriminator, respectively the discriminator associated with the power polynomial X^j. For fixed j and a, $Dickson_a(j, n)$ can be viewed as a function which maps the set of positive integers to itself. Let $Dickson_{j,a}(x)$ denote the number of elements $\leqslant x$ in the image of the function $Dickson_a(j, n)$. Put $D_j(x) = Dickson_{j,0}(x)$. The faster the growth of $Dickson_{j,a}(x)$, the stronger the "average permutational power" of the Dickson polynomial $g_j(X, a)$. Obviously $Dickson_{j,a}(x) \leqslant x$. For X (and only for X) equality always holds. Of all the Dickson polynomials, X is thus the best permuter.

In cases where j is even, $4 \nmid j$, an application of the prime number theorem for arithmetic progressions yields

$$Dickson_{j,a}(x) \sim \frac{3}{2}\mu_D(j)\frac{x}{\log x}, \qquad \text{where} \quad \mu_D(j) = \prod_{p \mid j,\, p>2} \frac{p-3}{p-1}$$

and

$$D_j(x) \sim \frac{3}{2}\mu_P(j)\frac{x}{\log x}, \qquad \text{where} \quad \mu_P(j) = \prod_{p \mid j,\, p>2} \frac{p-2}{p-1}.$$

(In case of the Dickson discriminator we make the additional assumption on j that $3 \nmid j$.) Clearly $0 \leqslant \mu_D(j), \mu_P(j) \leqslant 1$, and we note that μ_D and μ_P only depend on the squarefree part of j. We see that $\mu_D(j) \leqslant \mu_P(j)$. This is consistent with Remark 3.

Let $\mathbf{A} = \{a_1, ..., a_s\}$ be an ordered set of natural numbers with $1 \leqslant a_1 < a_2 < \cdots < a_s < m$, $(a_i, m) = 1$, $i = 1, ..., s$ and let $G_{\mathbf{A}}$ be the semigroup of natural numbers composed of only primes p satisfying $p \equiv a_i$

(mod m) for some $1 \leqslant i \leqslant s$. Then as x tends to infinity it can be shown that $G_{\mathbf{A}}(x)$, the number of elements in $G_{\mathbf{A}}$ not exceeding x, satisfies

$$G_{\mathbf{A}}(x) \sim c_A x(\log x)^{s/\phi(m)-1},$$

where c_A is some positive constant. Landau first obtained this result but we refer to Moree [15, Ch. 4, Thm. 2] for an elementary proof. For the number of squarefree elements in $G_{\mathbf{A}}$ not exceeding x, a similar result holds, although with a possibly different constant. As a consequence we find that for odd j,

$$D_j(x) \sim c_j x(\log x)^{\mu_P(j)-1},$$

and

$$Dickson_{j,a}(x) \sim c_{j,a} x(\log x)^{\mu_D(j)-1},$$

where c_j and $c_{j,a}$ are positive constants. So again μ_D and μ_P seem to be good measures for the average permutational power of $g_j(X, a)$ and X^j respectively. Notice that $\mu_D(j)$ and $\mu_P(j)$ are equal to the fraction of primitive residue classes b (mod j) such that $(j, b^2-1)|2$ and $(j, b-1)|2$, respectively. The constants B_j, C_j and L_j in Theorems 1 and 16 can be explicitly computed using an explicit form of the Burn–Titchmarsh theorem, provided the corresponding measure of permutability is close enough to 1. This gives another indication of the significance of these measures.

5. Open Problems

We conclude by raising several open problems designed to stimulate further work on Dickson discriminators. Since our work has not given a complete determination of $Dickson_a(j, n)$ for all a, j and n, we provide Table I with values for the Dickson discriminator $Dickson_1(j, n)$ for $1 \leqslant j \leqslant 25$; $1 \leqslant n \leqslant 20$. (As we have seen the a-dependence is not very strong.) We refer to Schumer and Steinig [21, p. 148] for a table containing the values of $D(j, n)$ for $2 \leqslant j \leqslant 30$; $1 \leqslant n \leqslant 20$.

Using property P6 of Lemma 7 it is easy to see that for fixed $j \geqslant 1$,

$$g_j(1, 1) \leqslant g_j(2, 1) < g_j(3, 1) < g_j(4, 1) < \cdots$$

We have $g_j(1, 1) = g_j(2, 1)$ precisely when j is divisible by 6 and so it follows that $Dickson_1(j, n) < \infty$ unless 6 divides j and $n \geqslant 2$ in which case we have $Dickson_1(j, 2) = \infty$. We note that $Dickson_1(j, 2) = 2$ unless 3 divides j, in which case $Dickson_1(j, 2) = 3$ if j is odd and ∞ otherwise.

Table I suggests that the behaviour of $Dickson_1(j, n)$ is completely different in the cases not covered by Theorems 9 and 16. In particular for fixed values of j covered by these results, $Dickson_1(j, n)$ grows linearly in n while in the cases not covered, the growth appears to be much faster.

We close by raising the following notion related to permutations. Let R be a finite commutative ring with identity. A polynomial $h(X) \in R[X]$ with the property that $h(x) = h(y)$ implies $x = y$ or $x = -y$ might be called a *weak permutation polynomial* over R. It can be shown that for j even and $k \geqslant 11$, $g_j(X, a)$ is a weak permutation polynomial over Z/kZ if and only if $(j, \psi_a(k)) = 2$ and $k = p$ or $k = 2p$, where p is prime. Thus we have a permutational interpretation of the condition appearing in (3) (cf. Section 1).

If R is an integral domain, the condition for a polynomial to be a weak permutation polynomial over R is equivalent to requiring that $h(x) = h(y)$ implies $x^2 = y^2$. This suggests the more general problem: for an arbitrary fixed integer $e \geqslant 1$ characterize the *e-permutation polynomials* $h(X)$ over R which are defined by the property that $h(x) = h(y)$ implies $x^e = y^e$. If $h(X)$ is an odd permutation polynomial over an integral domain R, then $h(X)^2$ is a 2-permutation polynomial. Thus X^{2j} with $(j, p^m - 1) = 1$ is a 2-permutation polynomial over F_{p^m} and $g_{2j}(X, a)$ with $(j, p^{2m} - 1) = 1$ is a 2-permutation polynomial over the field F_{p^m} $(p \nmid a)$. If $p \geqslant 7$ and $4 \mid j$, then it can be easily seen using Lidl and Niederreiter [13, Lemma 6.24] and P2 (two times) that $g_j(X, a)$ is not a 2-permutation polynomial over the prime field F_p.

Acknowledgments

The first author thanks the second author for inviting him to The Pennsylvania State University and for the hospitality received there. Furthermore he thanks Michael Zieve for his excellent comments on an earlier version and his contribution to a very stimulating e-mail correspondence. Both authors thank the referees for a number of helpful comments.

References

1. L. K. Arnold, S. J. Benkoski, and B. J. McCabe, The discriminator (a simple application of Bertrand's postulate), *Amer. Math. Mon.* **92** (1985), 275–277.
2. M. Barcau, A sharp estimate of the discriminator, *Nieuw Arch. Wisk.* **6** (1988), 247–250.
3. P. S. Bremser and J. Gomez-Calderon, Value sets of Dickson polynomials over Galois rings, *J. Number Theory* **38** (1991), 240–250.
4. P. S. Bremser, P. D. Schumer, and L. C. Washington, A note on the incongruence of consecutive integers to a fixed power, *J. Number Theory* **35** (1990), 105–108.
5. W.-S. Chou, J. Gomez-Calderon, and G. L. Mullen, Value sets of Dickson polynomials over finite fields, *J. Number Theory* **30** (1988), 334–344.

6. S. Chowla and H. Zassenhaus, Some conjectures concerning finite fields, *Norske Vid. Selsk. Forh. (Trondheim)* **41** (1968), 34–35.
7. S. D. Cohen, Proof of a conjecture of Chowla and Zassenhaus, *Canad. Math. Bull.* **33** (1990), 230–234.
8. H. Davenport, "Multiplicative Number Theory," 2nd ed., Springer-Verlag, Heidelberg, 1980.
9. M. Fried, On a conjecture of Schur, *Michigan Math. J.* **17** (1970), 41–55.
10. M. D. Fried, R. Guralnick, and J. Saxl, Schur covers and Carlitz's conjecture, *Israel J. Math.* **82** (1993), 157–225.
11. J. Gomez-Calderon, On the power polynomial x^d over Galois rings, *Rocky Mountain J. Math.* **22** (1992), 861–865.
12. R. Lidl, G. L. Mullen, and G. Turnwald, "Dickson Polynomials," Pitman Monographs & Surveys in Pure & Appl. Math., Vol. 65, Longman, Essex, England, 1993.
13. R. Lidl and H. Niederreiter, "Finite Fields," Encyclo. Math. Appl., Vol. 20, Addison–Wesley, Reading, MA, 1983. (Now distributed by Cambridge Univ. Press.)
14. B. R. McDonald, "Finite Rings with Identity," Dekker, New York, 1974.
15. P. Moree, "Psixyology and Diophantine Equations," Thesis, Leiden University, 1993.
16. P. Moree, The incongruence of consecutive polynomial values, *Finite Fields Appl.*, to appear.
17. P. Moree and H. Roskam, On an arithmetical function related to Euler's totient and the discriminator, *Fibonacci Quart.* **33** (1995), 332–340.
18. W. Nöbauer, Über Permutationspolynome und Permutationsfunktionen für Primzahlpotenzen, *Monatsh. Math.* **69** (1965), 230–238.
19. P. Ribenboim, "Catalan's Conjecture," Academic Press, San Diego, 1994.
20. P. Schumer, On the incongruence of consecutive cubes, *Math. Student* **58** (1990), 42–48.
21. P. Schumer and J. Steinig, On the incongruence of consecutive fourth powers, *Elem. Math.* **43** (1988), 145–149.
22. I. Schur, Über den Zusammenhang zwischen einen Problem der Zahlentheorie und einem Satz über algebraische Funktionen, *Sitzungsber. Preuss. Akad. Wiss. Berlin* (1923), 123–134.
23. D. Wan, A p-adic lifting lemma and its application to permutation polynomials, *in* "Finite Fields, Coding Theory, and Advances in Communications and Computing" (G. L. Mullen and P. J.-S. Shiue, Eds.), Lecture Notes in Pure and Applied Math., Vol. 141, pp. 209–216, Dekker, New York, 1993.
24. M. Zieve, A note on the discriminator, I and II, preprint.